FIG. 1

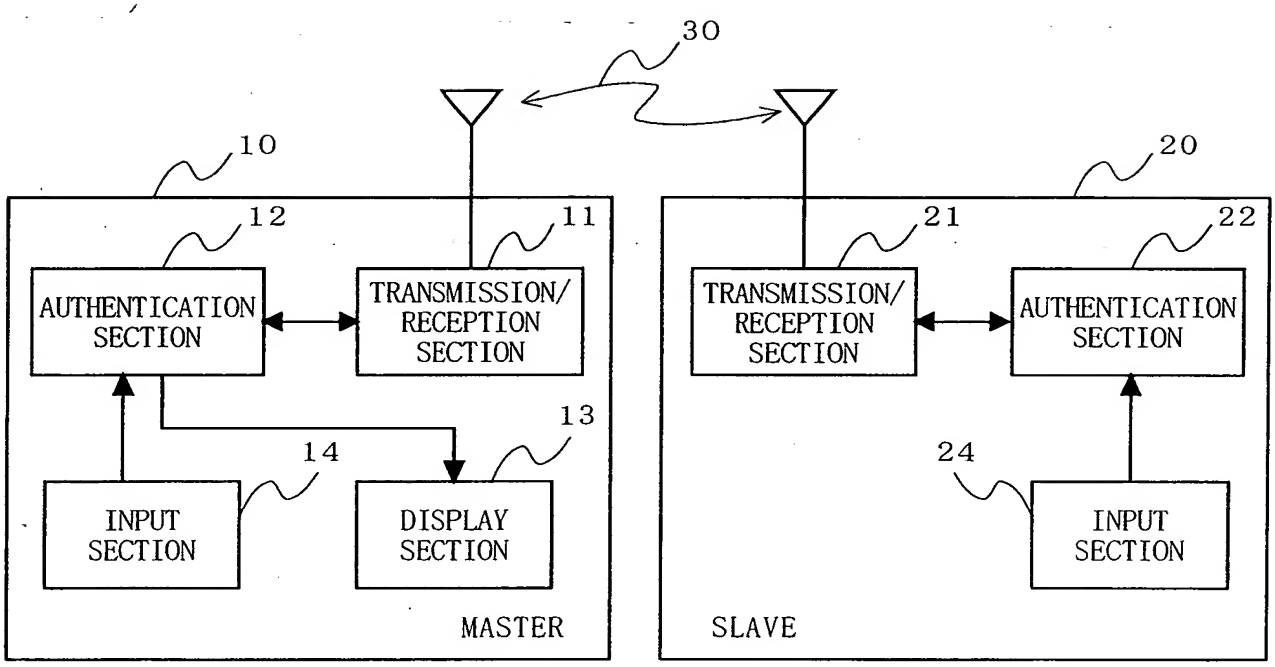

30
10
20
12
11
21
22
AUTHENTICATION SECTION
TRANSMISSION/ RECEPTION SECTION
TRANSMISSION/ RECEPTION SECTION
AUTHENTICATION SECTION
13
14
24
INPUT SECTION
DISPLAY SECTION
INPUT SECTION
MASTER
SLAVE

FIG. 2

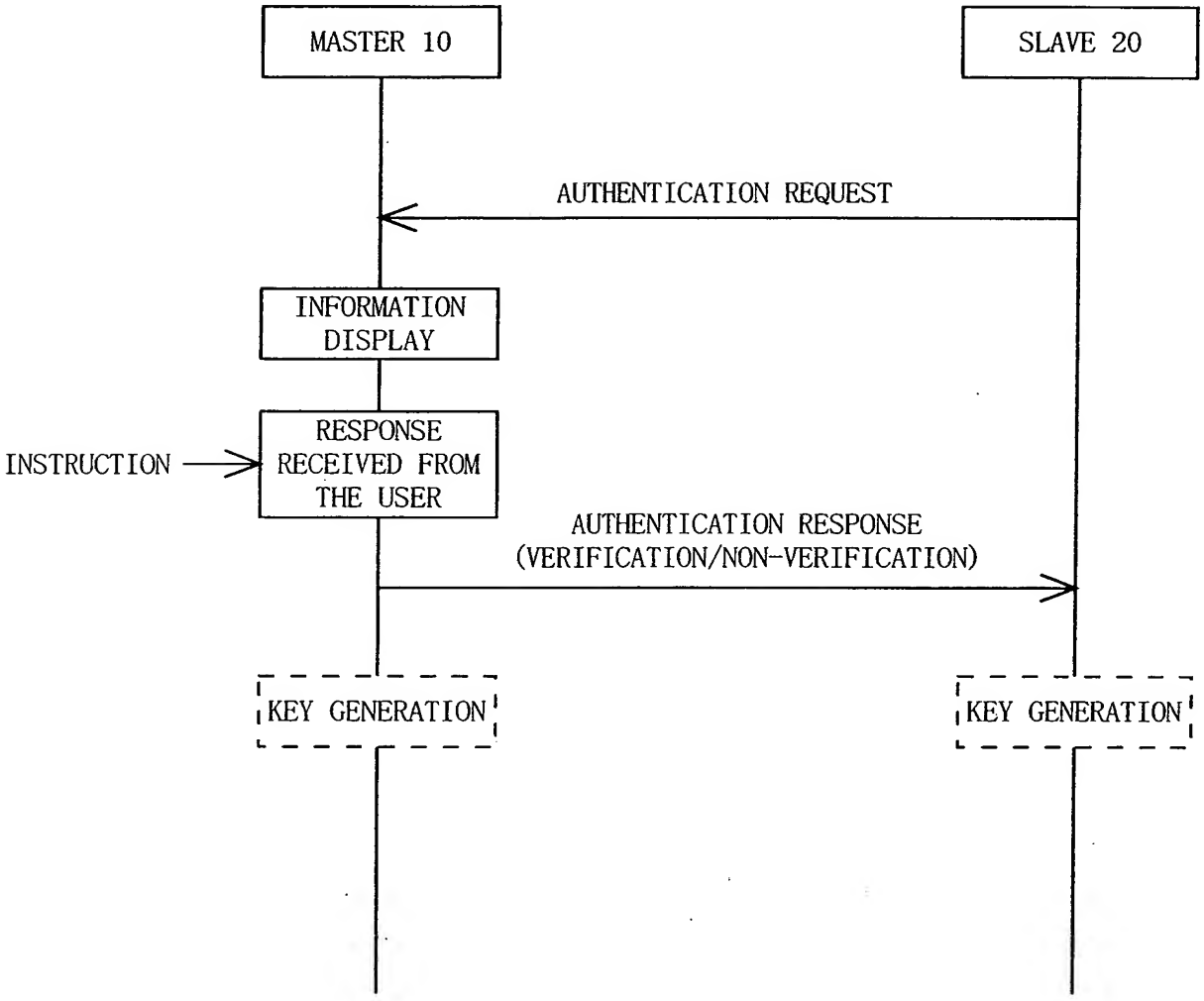

MASTER 10
SLAVE 20
AUTHENTICATION REQUEST
INFORMATION DISPLAY
INSTRUCTION
RESPONSE RECEIVED FROM THE USER
AUTHENTICATION RESPONSE (VERIFICATION/NON-VERIFICATION)
KEY GENERATION
KEY GENERATION

FIG. 3

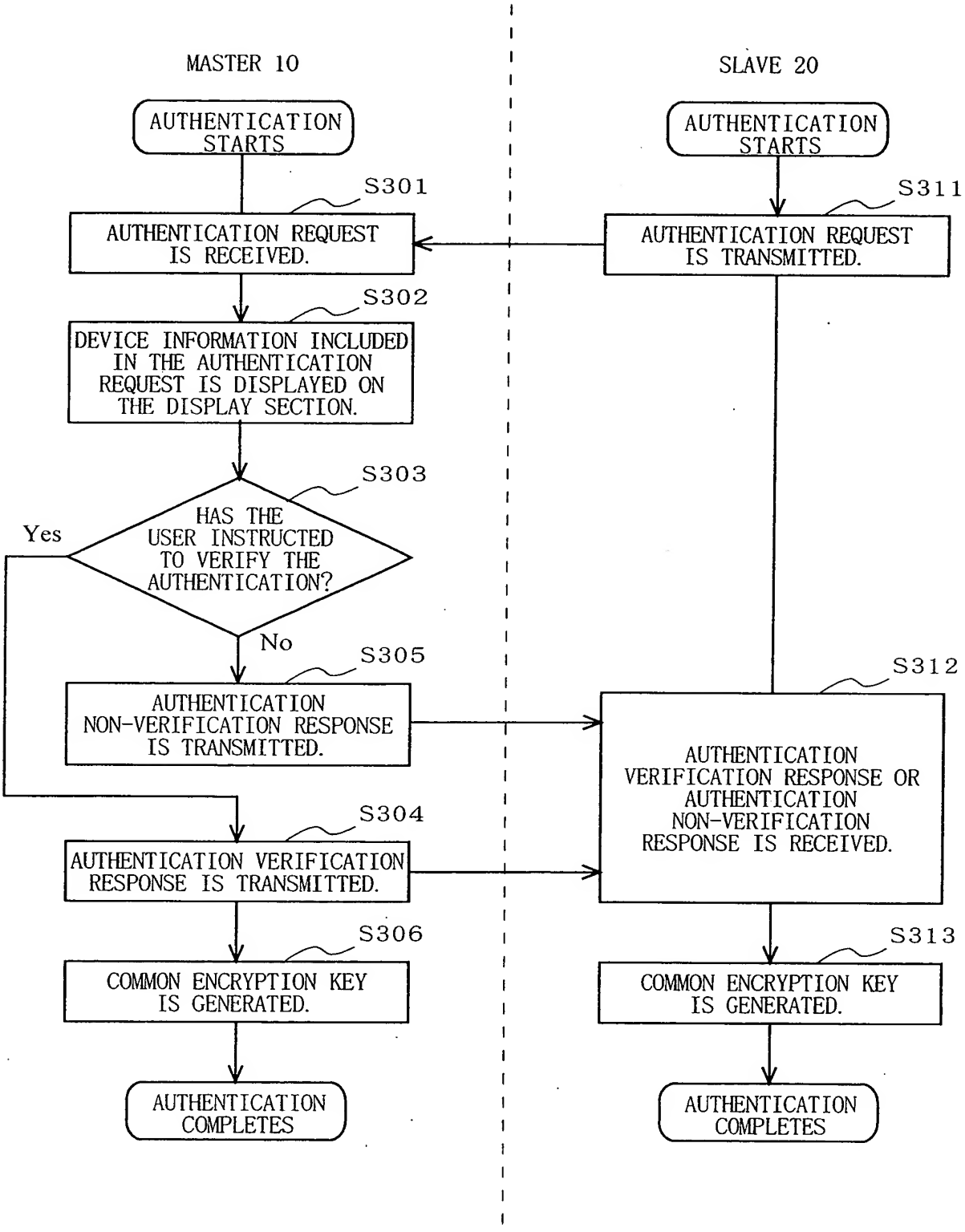

MASTER 10
SLAVE 20
AUTHENTICATION STARTS
AUTHENTICATION STARTS
S301
S311
AUTHENTICATION REQUEST IS RECEIVED.
AUTHENTICATION REQUEST IS TRANSMITTED.
S302
DEVICE INFORMATION INCLUDED IN THE AUTHENTICATION REQUEST IS DISPLAYED ON THE DISPLAY SECTION.
S303
Yes
HAS THE USER INSTRUCTED TO VERIFY THE AUTHENTICATION?
No
S305
S312
AUTHENTICATION NON-VERIFICATION RESPONSE IS TRANSMITTED.
AUTHENTICATION VERIFICATION RESPONSE OR AUTHENTICATION NON-VERIFICATION RESPONSE IS RECEIVED.
S304
AUTHENTICATION VERIFICATION RESPONSE IS TRANSMITTED.
S306
S313
COMMON ENCRYPTION KEY IS GENERATED.
COMMON ENCRYPTION KEY IS GENERATED.
AUTHENTICATION COMPLETES
AUTHENTICATION COMPLETES

FIG. 4A

AUTHENTICATION REQUEST
IDENTIFICATION NUMBER (IDs)
PUBLIC KEY (PubKey)
ENCRYPTION ALGORITHM (EncAlg)
[ELECTRONIC SIGNATURE (Sign), ELECTRONIC SIGNATURE ALGORITHM (SigAlg)]

FIG. 4B

AUTHENTICATION RESPONSE
IDENTIFICATION NUMBER (PubKey (IDm))
RANDOM NUMBER (PubKey(N))

FIG. 5A

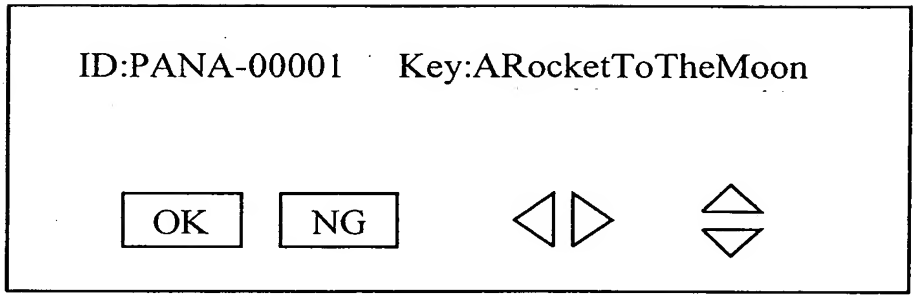

ID:PANA-00001 Key:ARocketToTheMoon
OK
NG

FIG. 5B

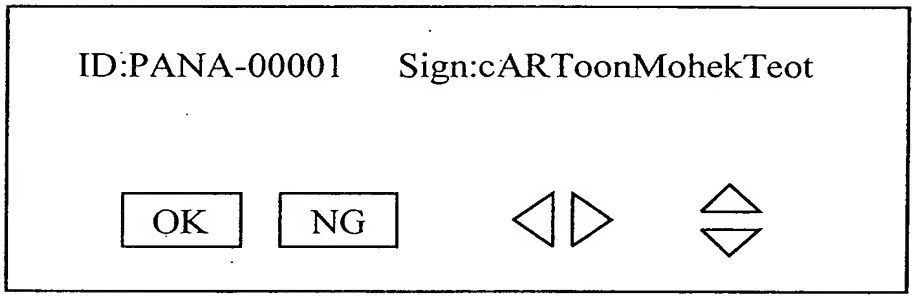

ID:PANA-00001 Sign:cARToonMohekTeot
OK
NG

FIG. 6

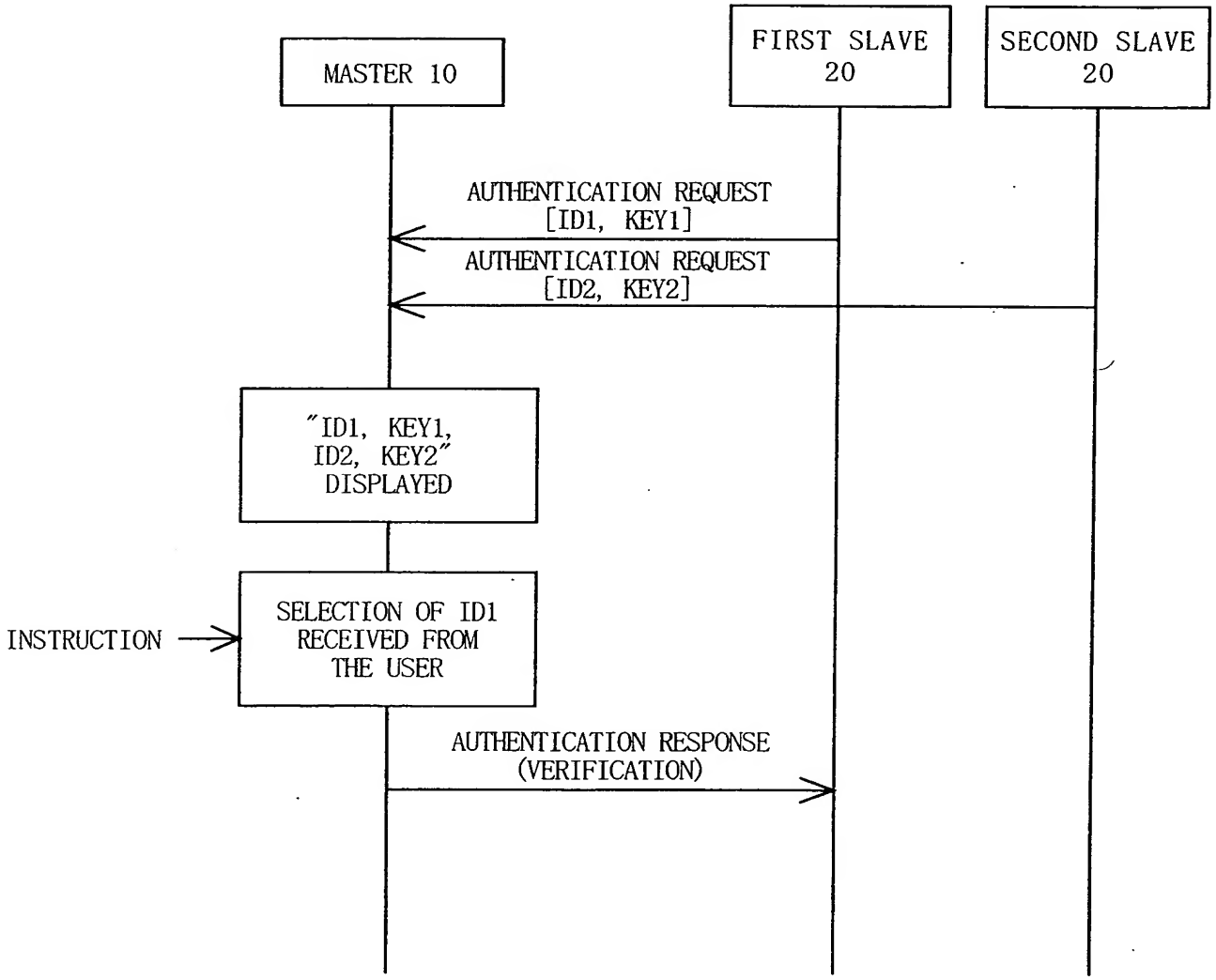

MASTER 10
FIRST SLAVE 20
SECOND SLAVE 20
AUTHENTICATION REQUEST [ID1, KEY1]
AUTHENTICATION REQUEST [ID2, KEY2]
"ID1, KEY1, ID2, KEY2" DISPLAYED
INSTRUCTION
SELECTION OF ID1 RECEIVED FROM THE USER
AUTHENTICATION RESPONSE (VERIFICATION)

FIG. 7

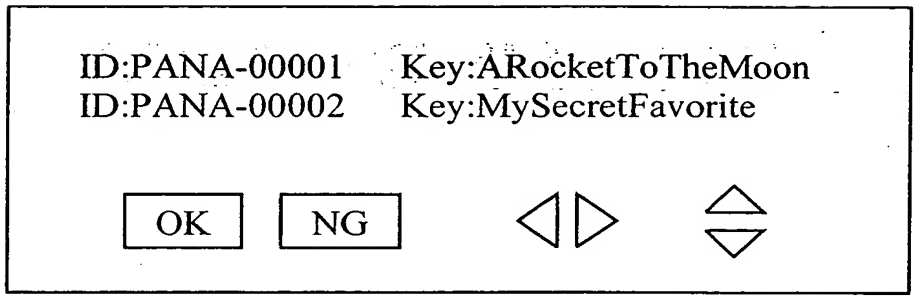

ID:PANA-00001 Key:ARocketToTheMoon
ID:PANA-00002 Key:MySecretFavorite
OK
NG

FIG. 8

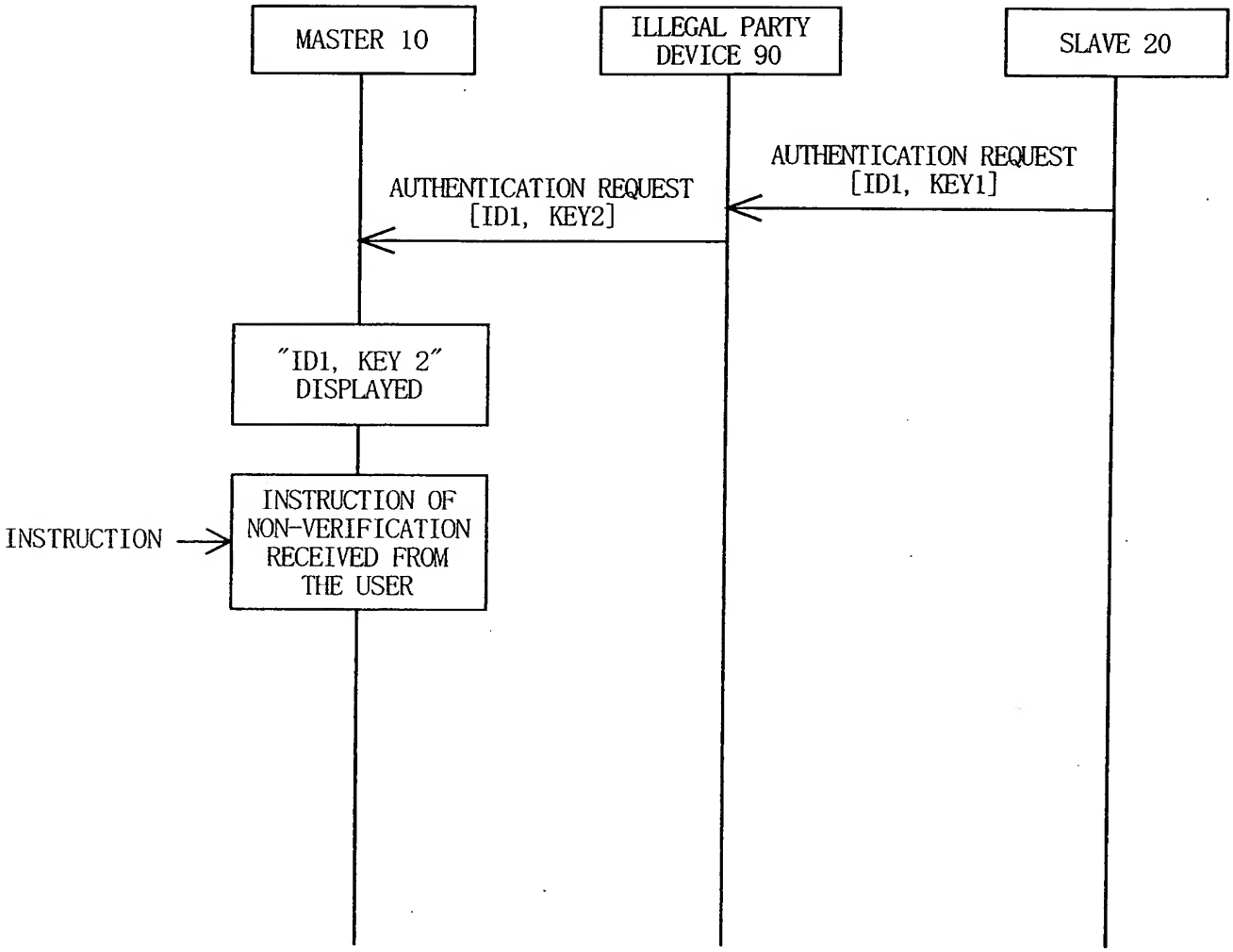

MASTER 10
ILLEGAL PARTY DEVICE 90
SLAVE 20
AUTHENTICATION REQUEST [ID1, KEY1]
AUTHENTICATION REQUEST [ID1, KEY2]
"ID1, KEY 2" DISPLAYED
INSTRUCTION
INSTRUCTION OF NON-VERIFICATION RECEIVED FROM THE USER

FIG. 9

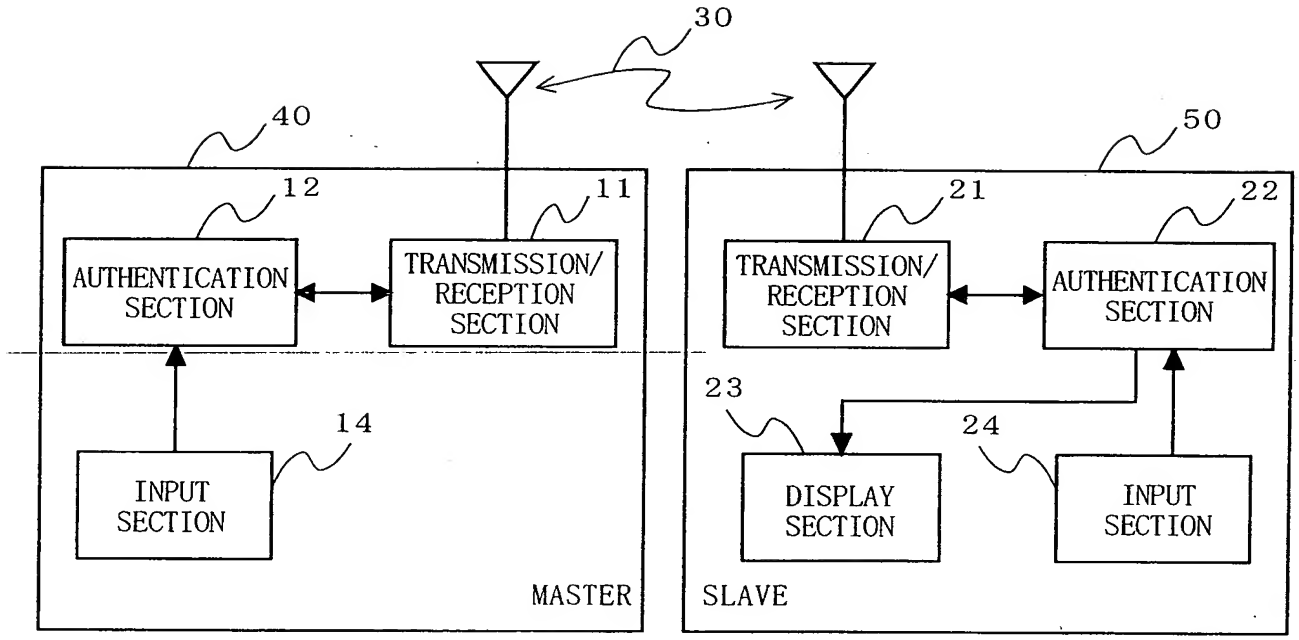

30
40
50
12
11
21
22
AUTHENTICATION SECTION
TRANSMISSION/ RECEPTION SECTION
TRANSMISSION/ RECEPTION SECTION
AUTHENTICATION SECTION
23
24
14
INPUT SECTION
DISPLAY SECTION
INPUT SECTION
MASTER
SLAVE

FIG. 10

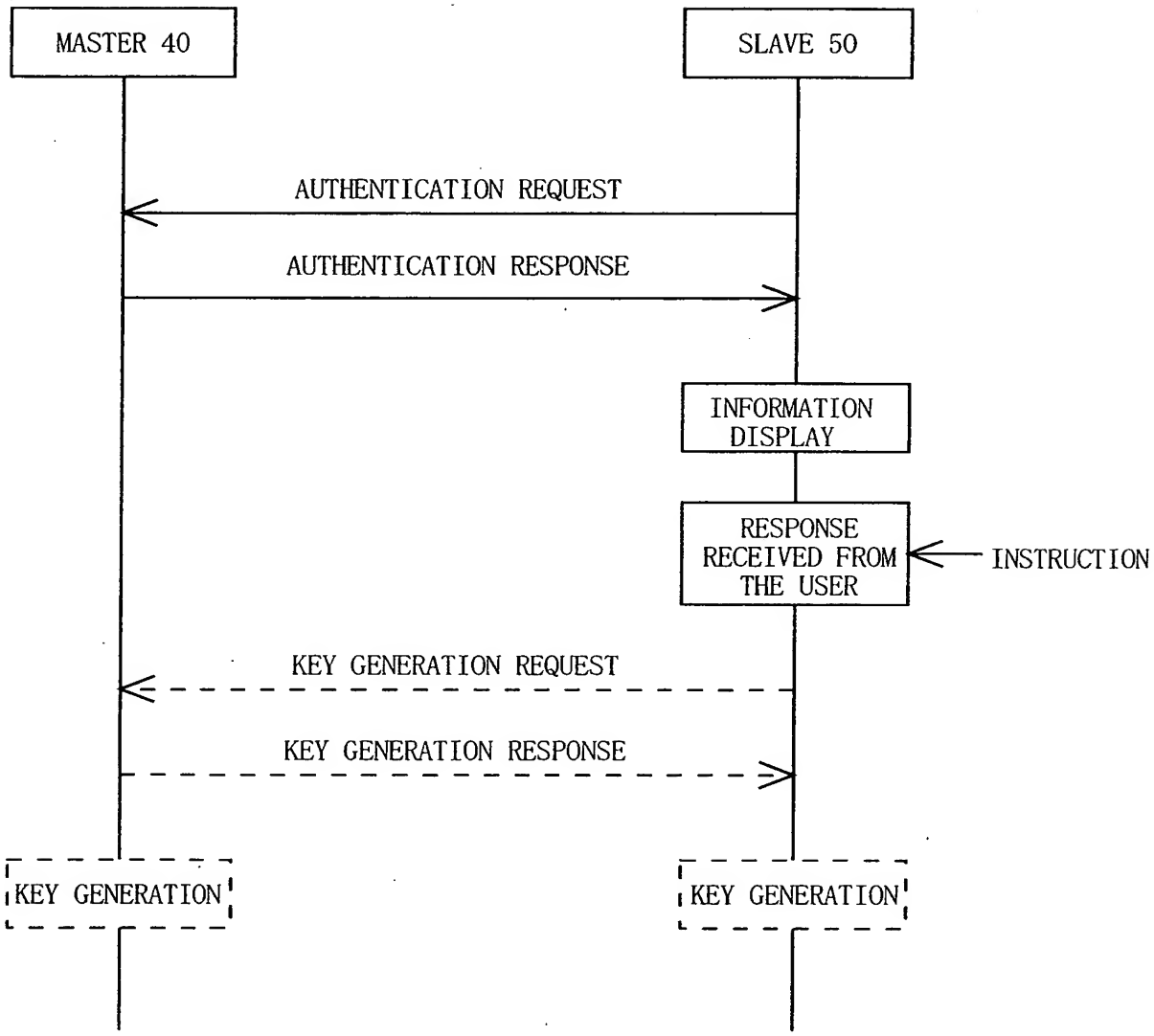

MASTER 40
SLAVE 50
AUTHENTICATION REQUEST
AUTHENTICATION RESPONSE
INFORMATION DISPLAY
RESPONSE RECEIVED FROM THE USER
INSTRUCTION
KEY GENERATION REQUEST
KEY GENERATION RESPONSE
KEY GENERATION
KEY GENERATION

FIG. 11

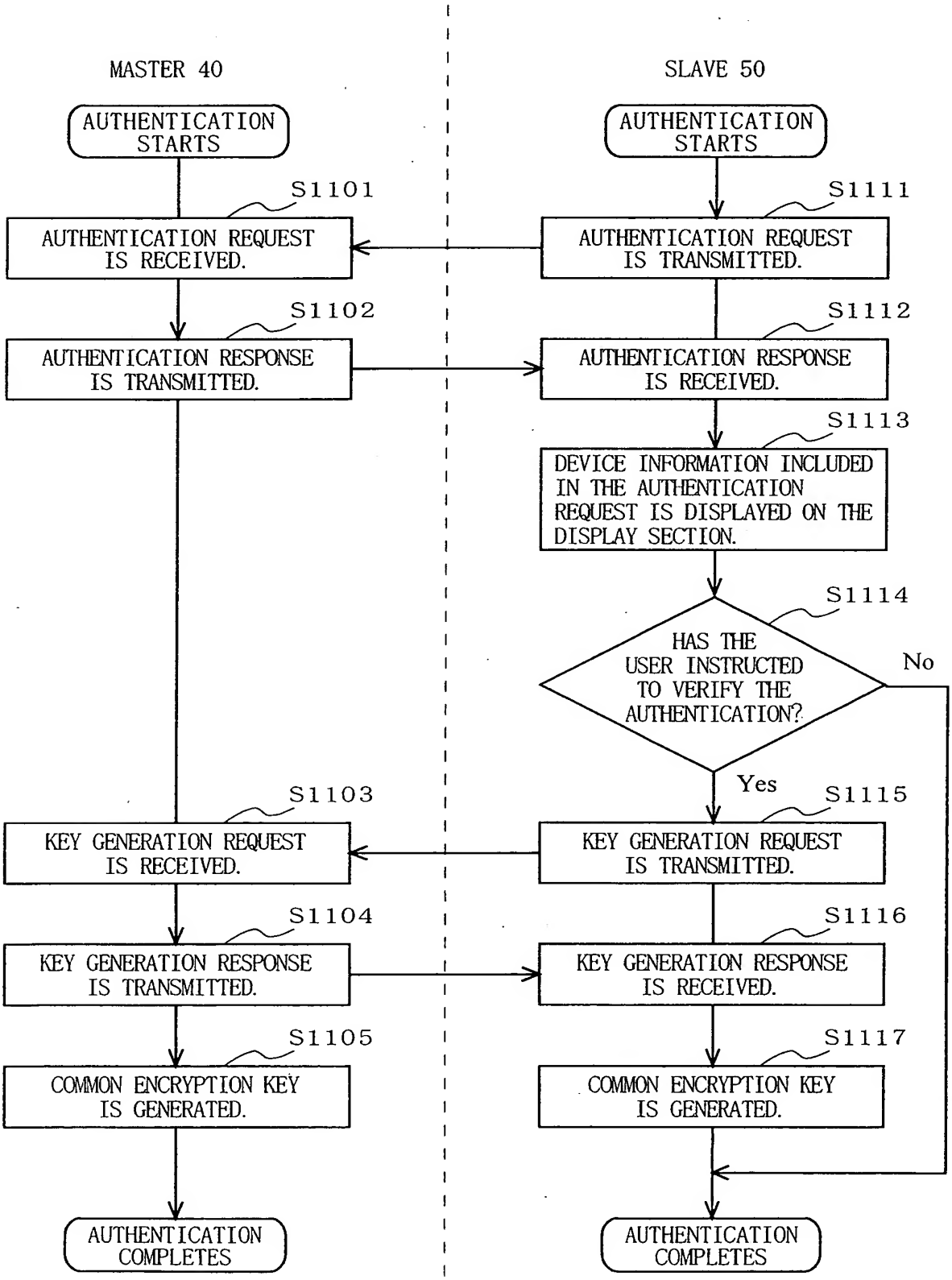

MASTER 40
SLAVE 50
AUTHENTICATION STARTS
AUTHENTICATION STARTS
S1101
AUTHENTICATION REQUEST IS RECEIVED.
S1111
AUTHENTICATION REQUEST IS TRANSMITTED.
S1102
AUTHENTICATION RESPONSE IS TRANSMITTED.
S1112
AUTHENTICATION RESPONSE IS RECEIVED.
S1113
DEVICE INFORMATION INCLUDED IN THE AUTHENTICATION REQUEST IS DISPLAYED ON THE DISPLAY SECTION.
S1114
HAS THE USER INSTRUCTED TO VERIFY THE AUTHENTICATION?
No
Yes
S1103
KEY GENERATION REQUEST IS RECEIVED.
S1115
KEY GENERATION REQUEST IS TRANSMITTED.
S1104
KEY GENERATION RESPONSE IS TRANSMITTED.
S1116
KEY GENERATION RESPONSE IS RECEIVED.
S1105
COMMON ENCRYPTION KEY IS GENERATED.
S1117
COMMON ENCRYPTION KEY IS GENERATED.
AUTHENTICATION COMPLETES
AUTHENTICATION COMPLETES

FIG. 12A

AUTHENTICATION REQUEST
IDENTIFICATION NUMBER (IDs)

FIG. 12B

AUTHENTICATION RESPONSE
IDENTIFICATION NUMBER (IDm)
PUBLIC KEY OF THE MASTER (PubKeyM)
ENCRYPTION ALGORITHM (EncAlg)
[ELECTRONIC SIGNATURE (SignM), ELECTRONIC SIGNATURE ALGORITHM (SigAlg)]

FIG. 12C

KEY GENERATION REQUEST
PUBLIC KEY OF THE SLAVE (PubKeyM(PubKeyS))
RANDOM NUMBER 1 (PubKeyM(Ns))

FIG. 12D

KEY GENERATION RESPONSE
RANDOM NUMBER 2 (PubKeyS(Nm))

FIG. 13

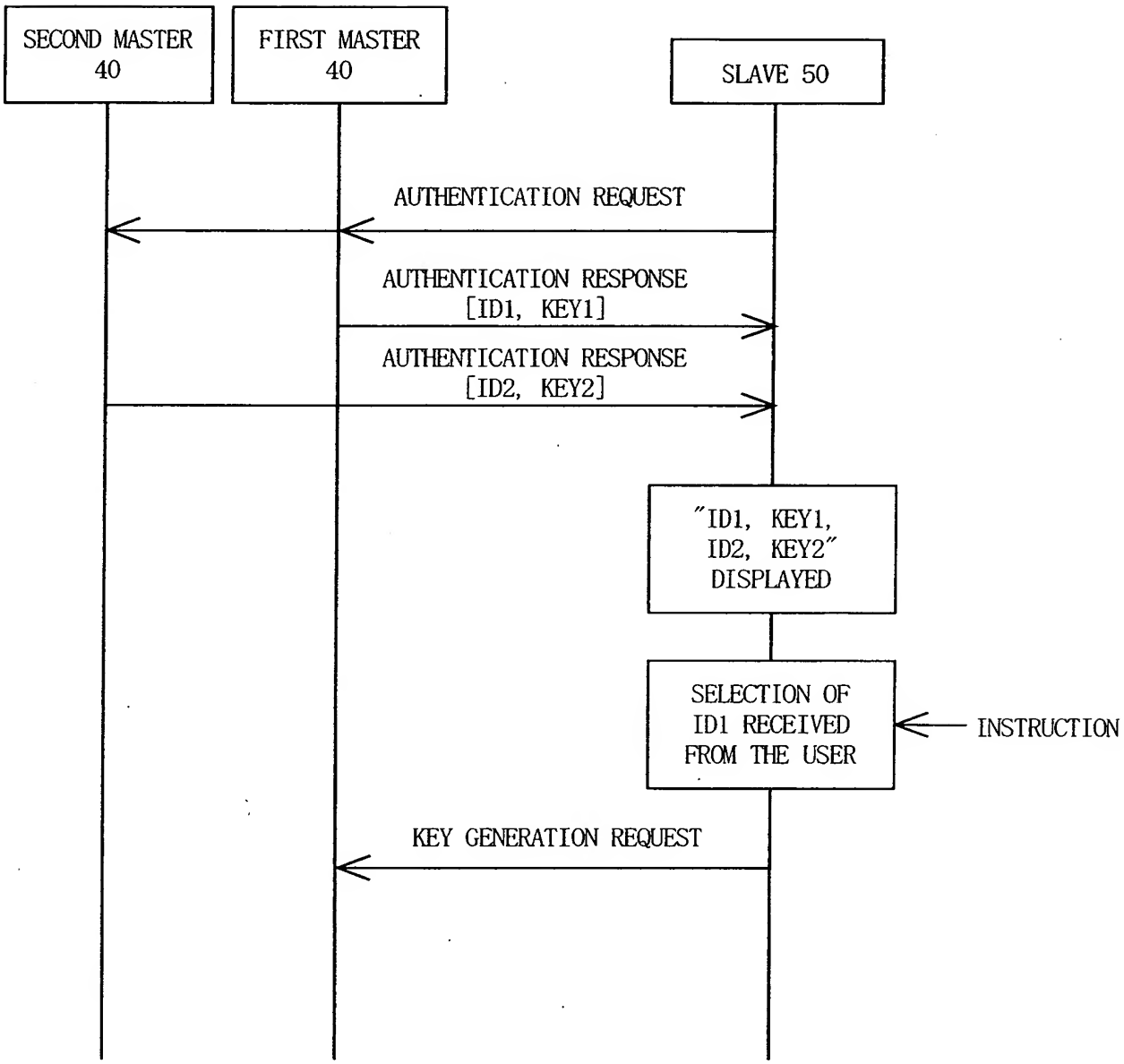

SECOND MASTER 40
FIRST MASTER 40
SLAVE 50
AUTHENTICATION REQUEST
AUTHENTICATION RESPONSE [ID1, KEY1]
AUTHENTICATION RESPONSE [ID2, KEY2]
"ID1, KEY1, ID2, KEY2" DISPLAYED
SELECTION OF ID1 RECEIVED FROM THE USER
INSTRUCTION
KEY GENERATION REQUEST

FIG. 14

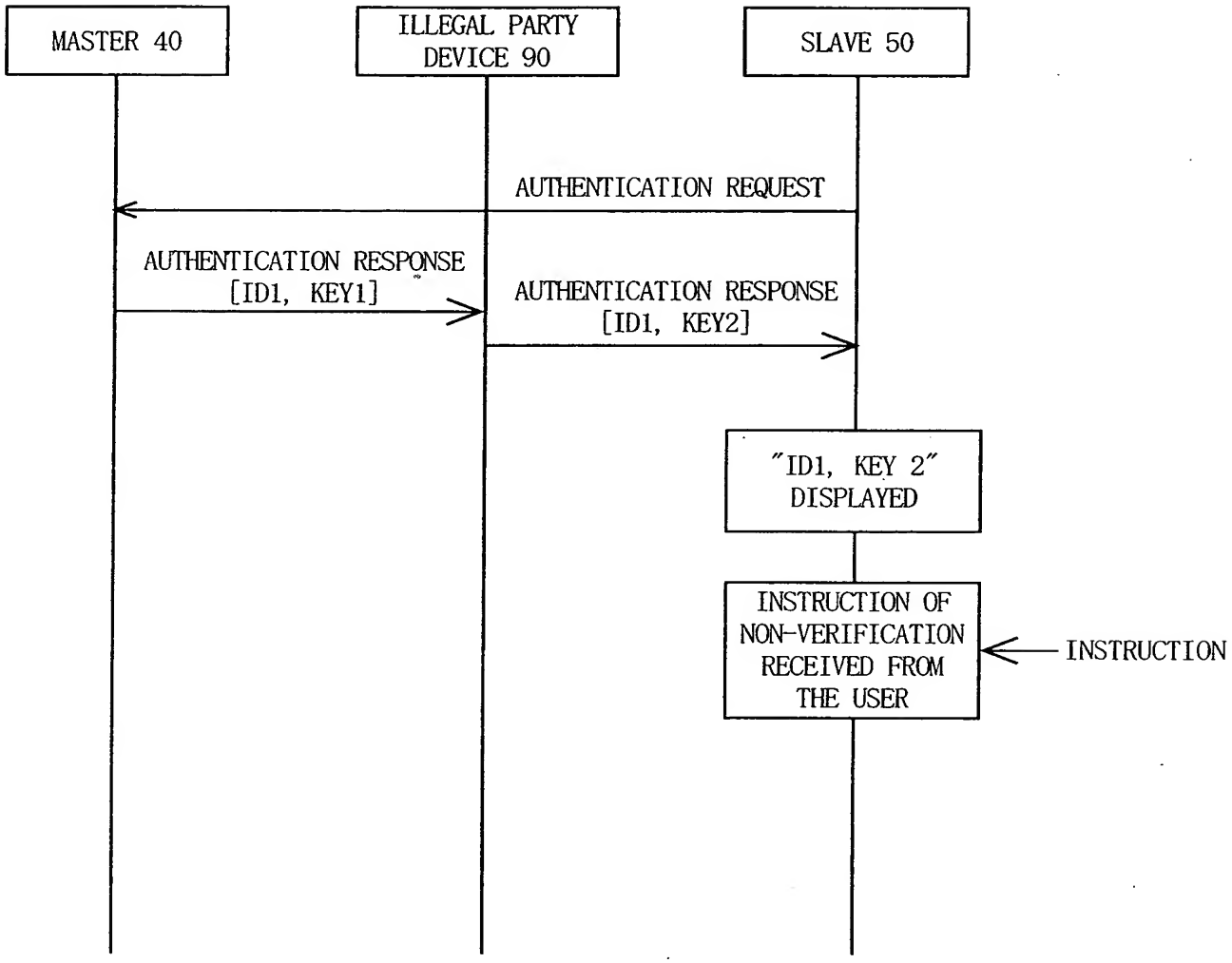

MASTER 40
ILLEGAL PARTY DEVICE 90
SLAVE 50
AUTHENTICATION REQUEST
AUTHENTICATION RESPONSE [ID1, KEY1]
AUTHENTICATION RESPONSE [ID1, KEY2]
"ID1, KEY 2" DISPLAYED
INSTRUCTION OF NON-VERIFICATION RECEIVED FROM THE USER
INSTRUCTION

FIG. 15

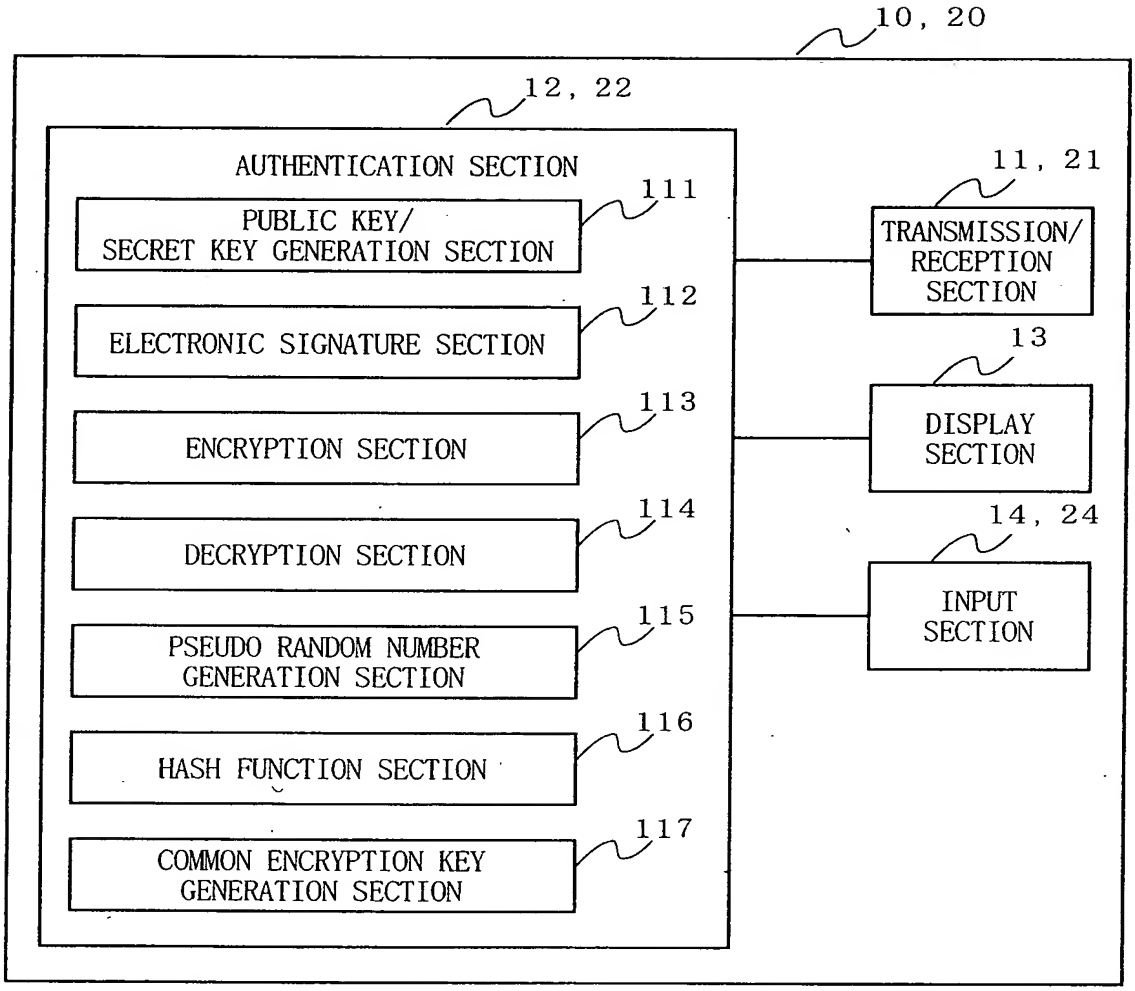

10, 20
12, 22
AUTHENTICATION SECTION
111
PUBLIC KEY/
SECRET KEY GENERATION SECTION
112
ELECTRONIC SIGNATURE SECTION
113
ENCRYPTION SECTION
114
DECRYPTION SECTION
115
PSEUDO RANDOM NUMBER
GENERATION SECTION
116
HASH FUNCTION SECTION
117
COMMON ENCRYPTION KEY
GENERATION SECTION
11, 21
TRANSMISSION/
RECEPTION
SECTION
13
DISPLAY
SECTION
14, 24
INPUT
SECTION

FIG. 16

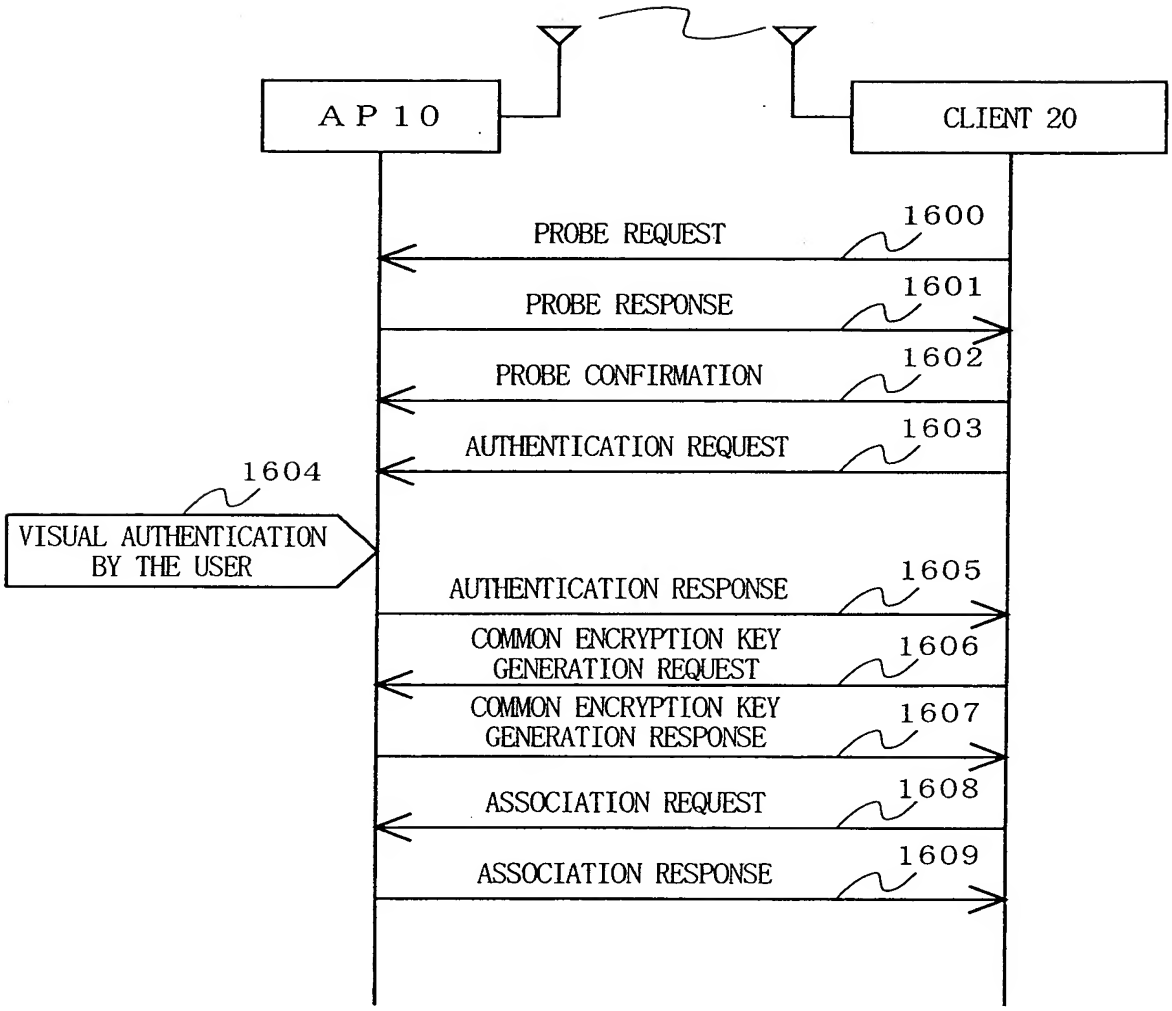

AP 10
CLIENT 20
PROBE REQUEST
1600
PROBE RESPONSE
1601
PROBE CONFIRMATION
1602
AUTHENTICATION REQUEST
1603
1604
VISUAL AUTHENTICATION BY THE USER
AUTHENTICATION RESPONSE
1605
COMMON ENCRYPTION KEY GENERATION REQUEST
1606
COMMON ENCRYPTION KEY GENERATION RESPONSE
1607
ASSOCIATION REQUEST
1608
ASSOCIATION RESPONSE
1609

FIG. 17

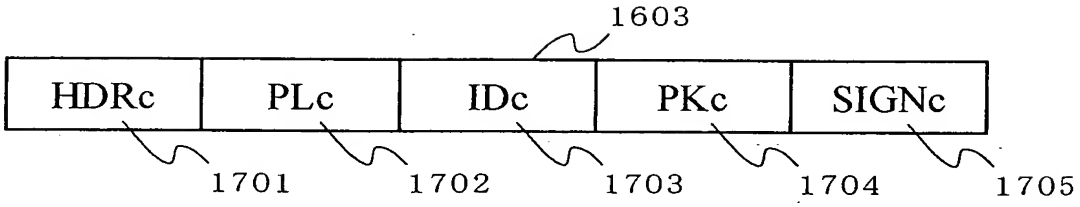


FIG. 18

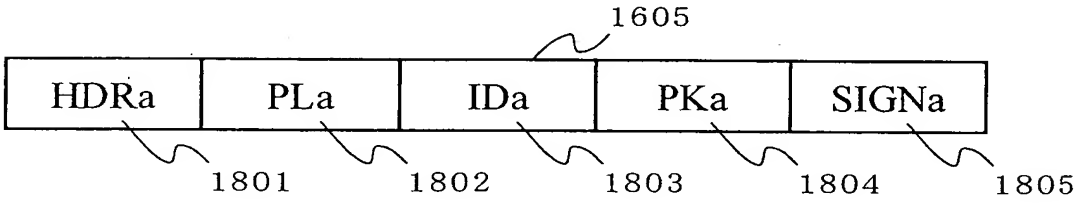


FIG. 19

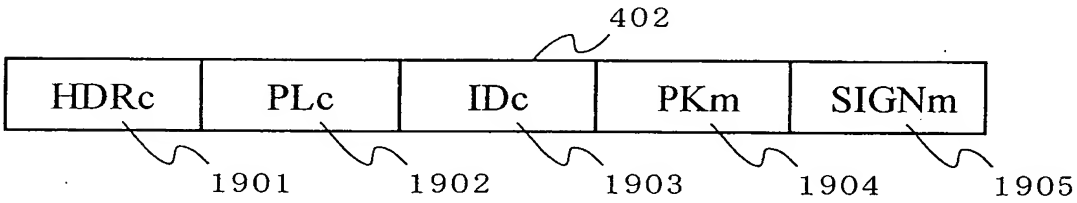


FIG. 20

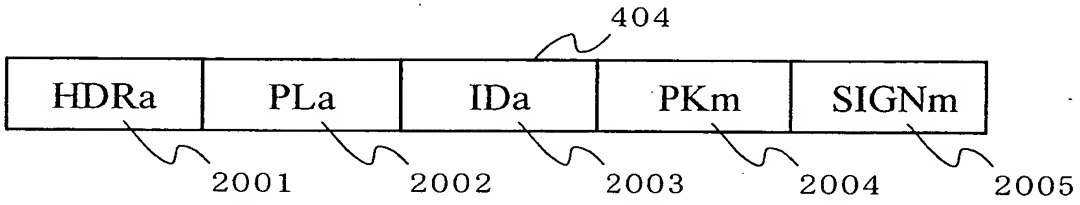


FIG. 21

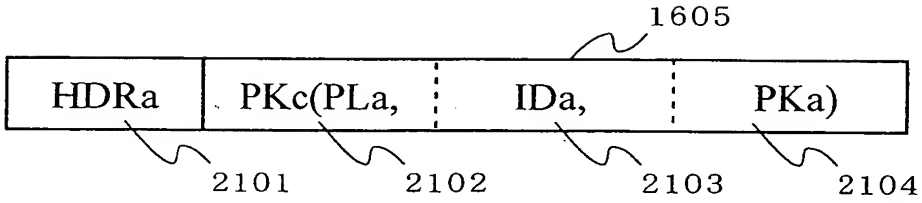


FIG. 22

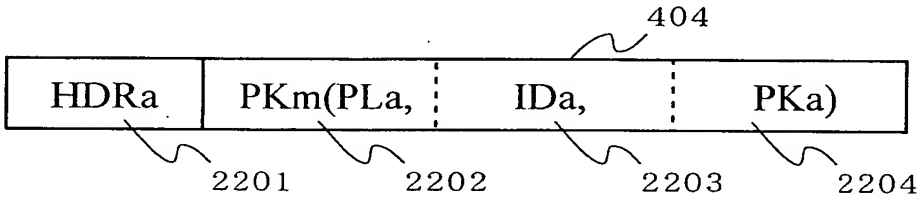


FIG. 23

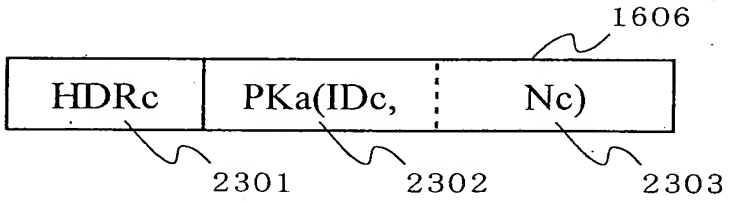


FIG. 24

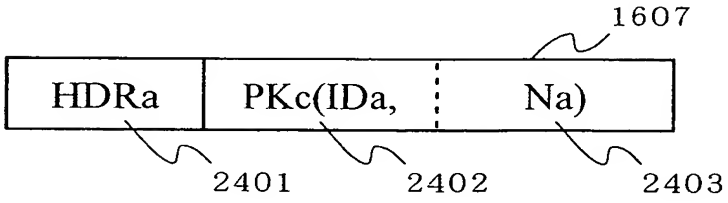


FIG. 25

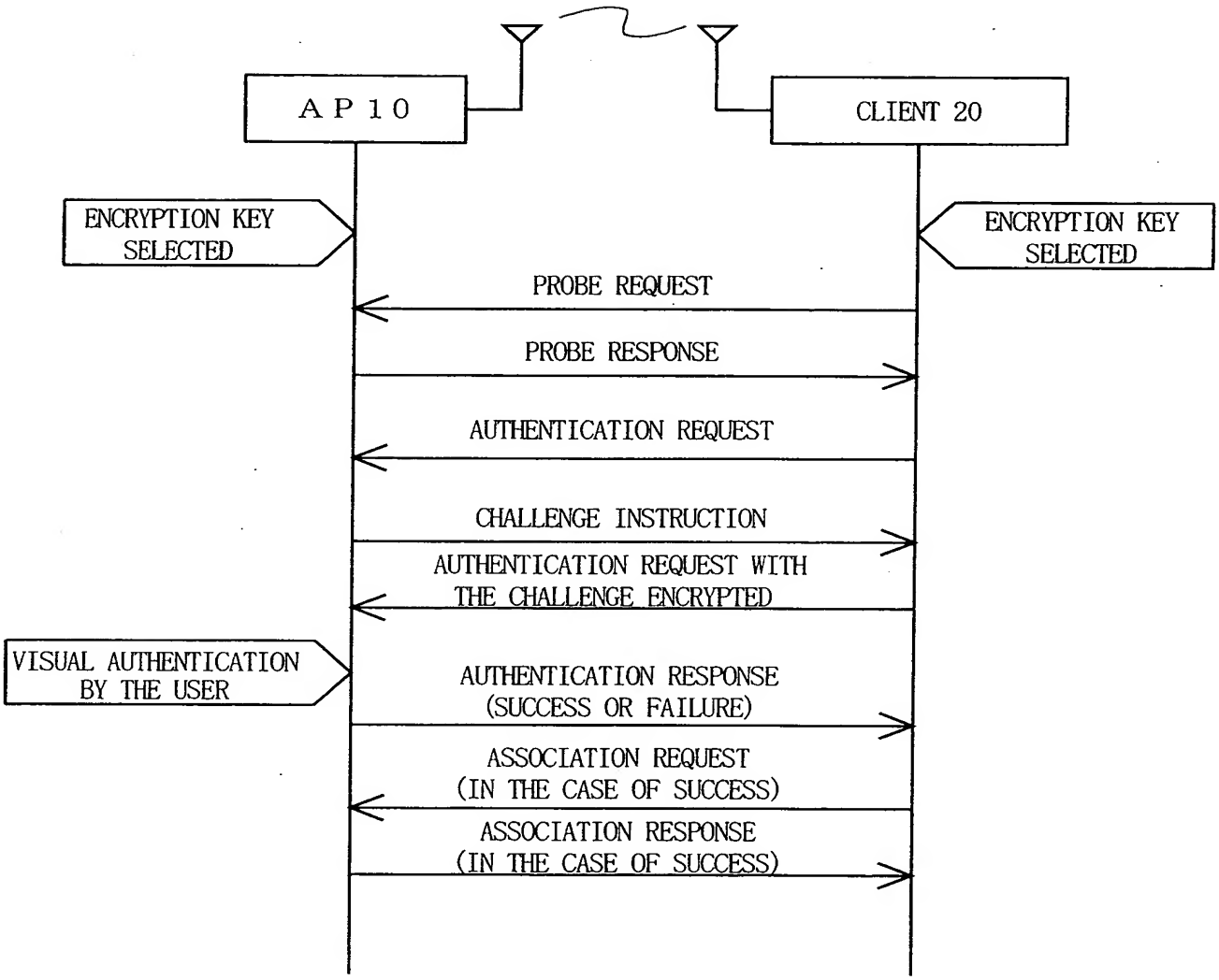

AP 10
CLIENT 20
ENCRYPTION KEY SELECTED
ENCRYPTION KEY SELECTED
PROBE REQUEST
PROBE RESPONSE
AUTHENTICATION REQUEST
CHALLENGE INSTRUCTION
AUTHENTICATION REQUEST WITH THE CHALLENGE ENCRYPTED
VISUAL AUTHENTICATION BY THE USER
AUTHENTICATION RESPONSE (SUCCESS OR FAILURE)
ASSOCIATION REQUEST (IN THE CASE OF SUCCESS)
ASSOCIATION RESPONSE (IN THE CASE OF SUCCESS)

FIG. 26

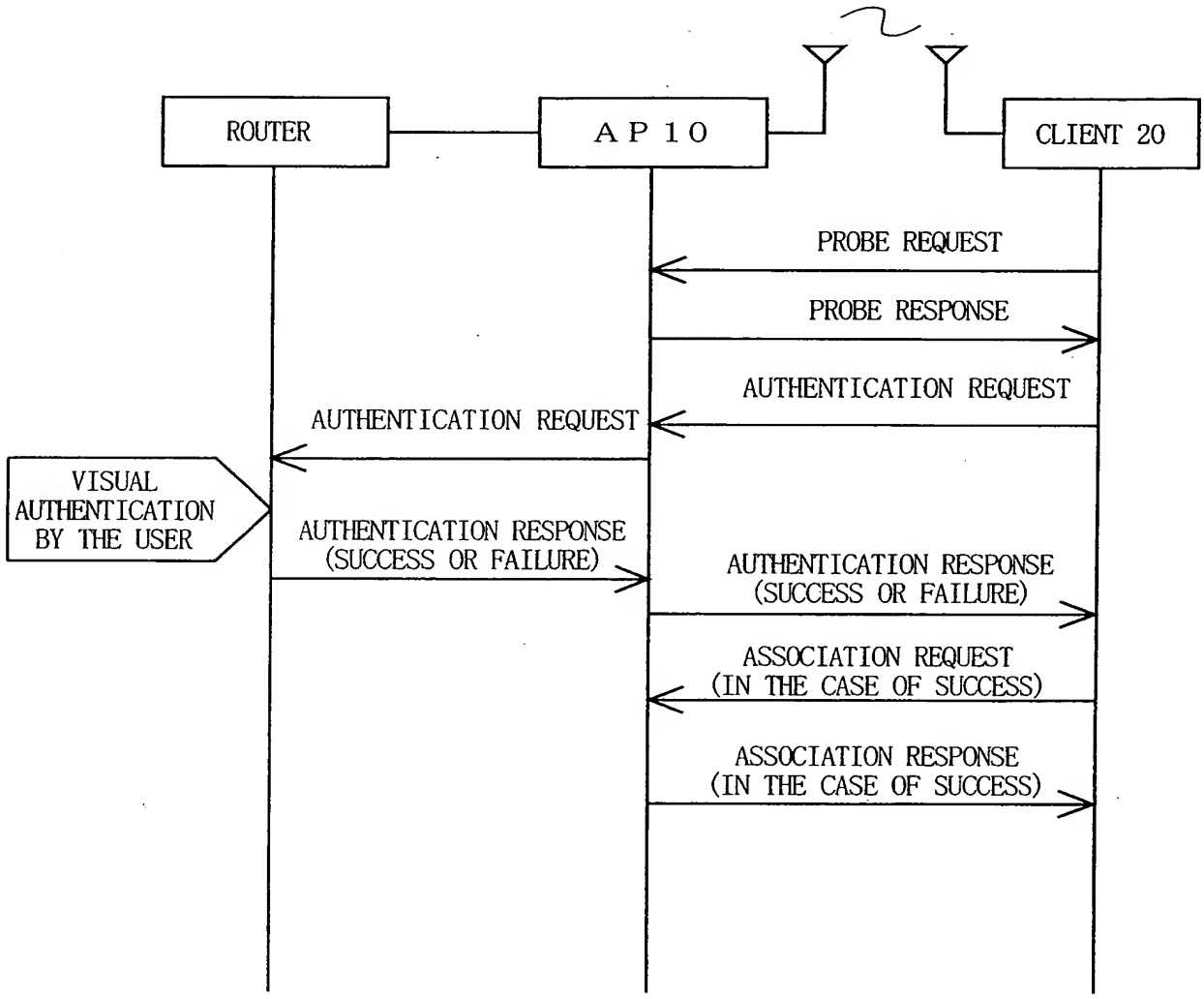

ROUTER
AP 10
CLIENT 20
PROBE REQUEST
PROBE RESPONSE
AUTHENTICATION REQUEST
AUTHENTICATION REQUEST
VISUAL AUTHENTICATION BY THE USER
AUTHENTICATION RESPONSE (SUCCESS OR FAILURE)
AUTHENTICATION RESPONSE (SUCCESS OR FAILURE)
ASSOCIATION REQUEST (IN THE CASE OF SUCCESS)
ASSOCIATION RESPONSE (IN THE CASE OF SUCCESS)

FIG. 27

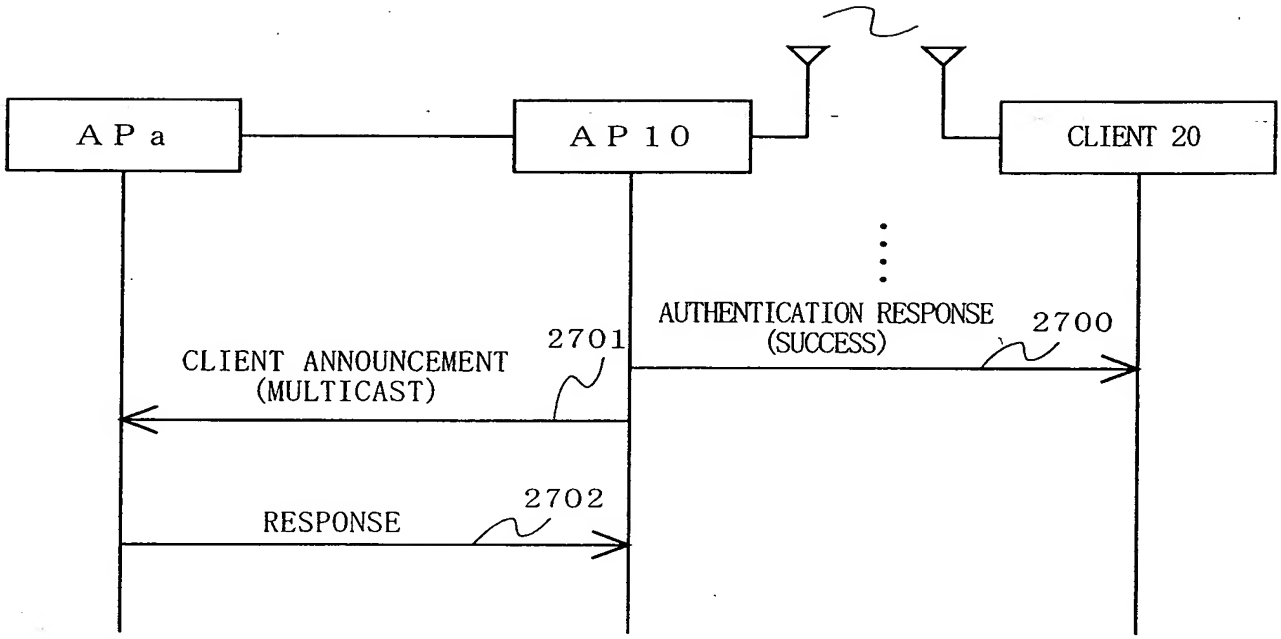

AP a
AP 10
CLIENT 20
AUTHENTICATION RESPONSE
(SUCCESS)
2700
2701
CLIENT ANNOUNCEMENT
(MULTICAST)
2702
RESPONSE

FIG. 28

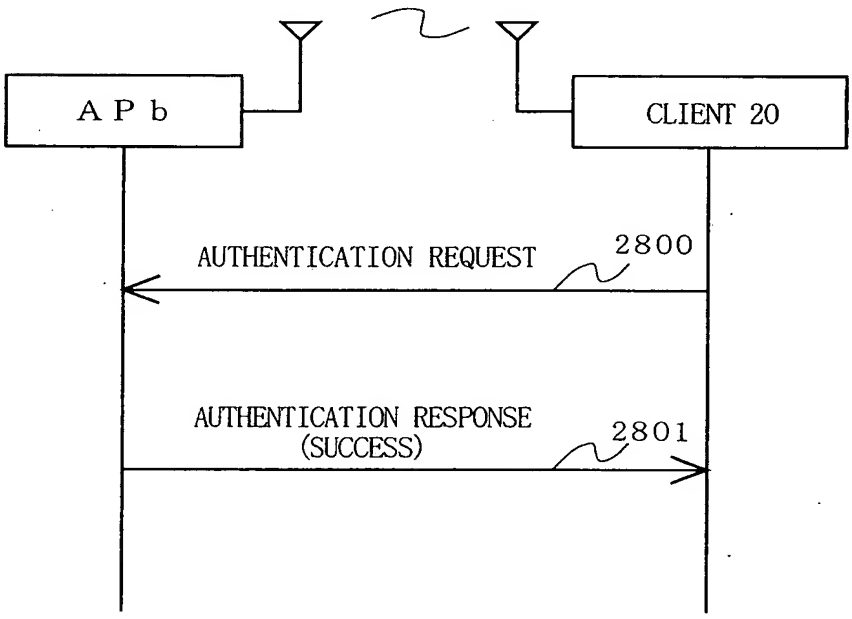

AP b
CLIENT 20
AUTHENTICATION REQUEST
2800
AUTHENTICATION RESPONSE
(SUCCESS)
2801

FIG. 29

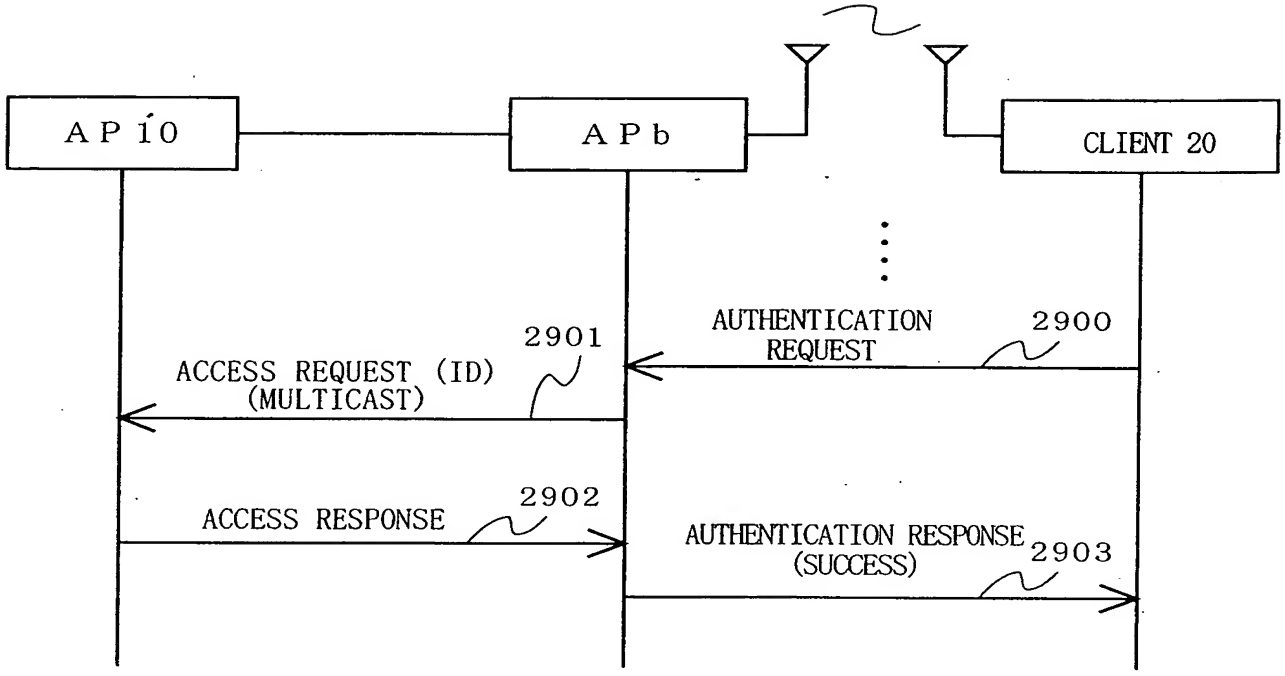

AP 10
APb
CLIENT 20
AUTHENTICATION REQUEST
2900
2901
ACCESS REQUEST (ID) (MULTICAST)
2902
ACCESS RESPONSE
AUTHENTICATION RESPONSE (SUCCESS)
2903

FIG. 30

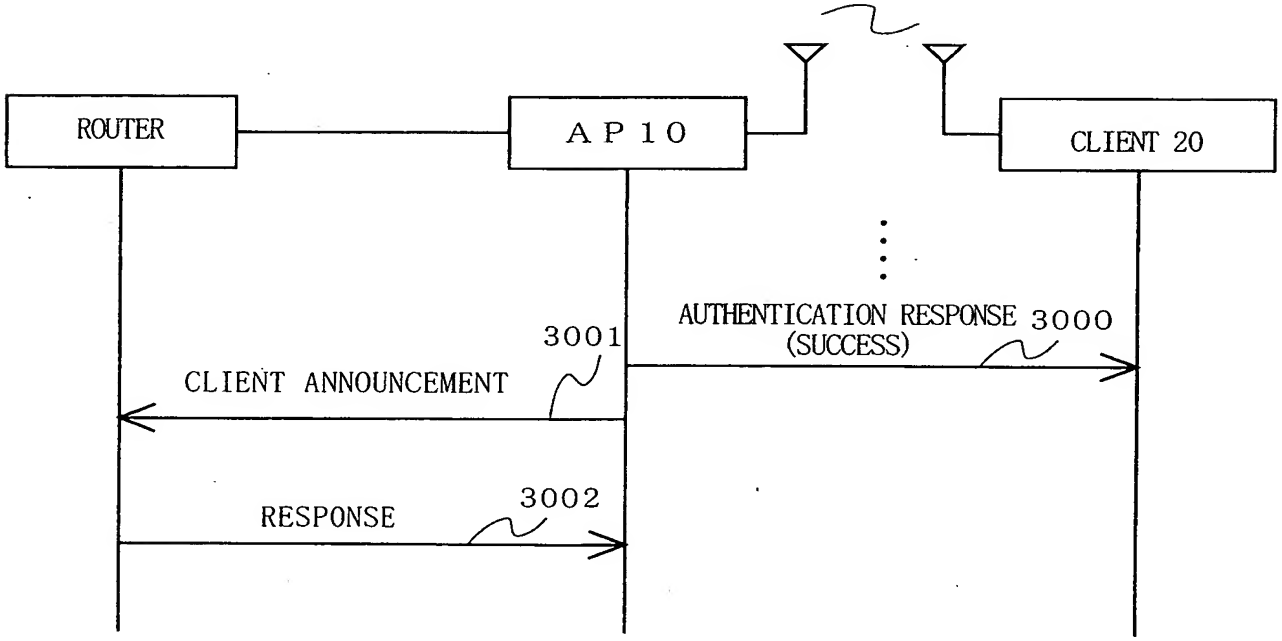

ROUTER
AP 10
CLIENT 20
AUTHENTICATION RESPONSE (SUCCESS)
3000
3001
CLIENT ANNOUNCEMENT
3002
RESPONSE

FIG. 31

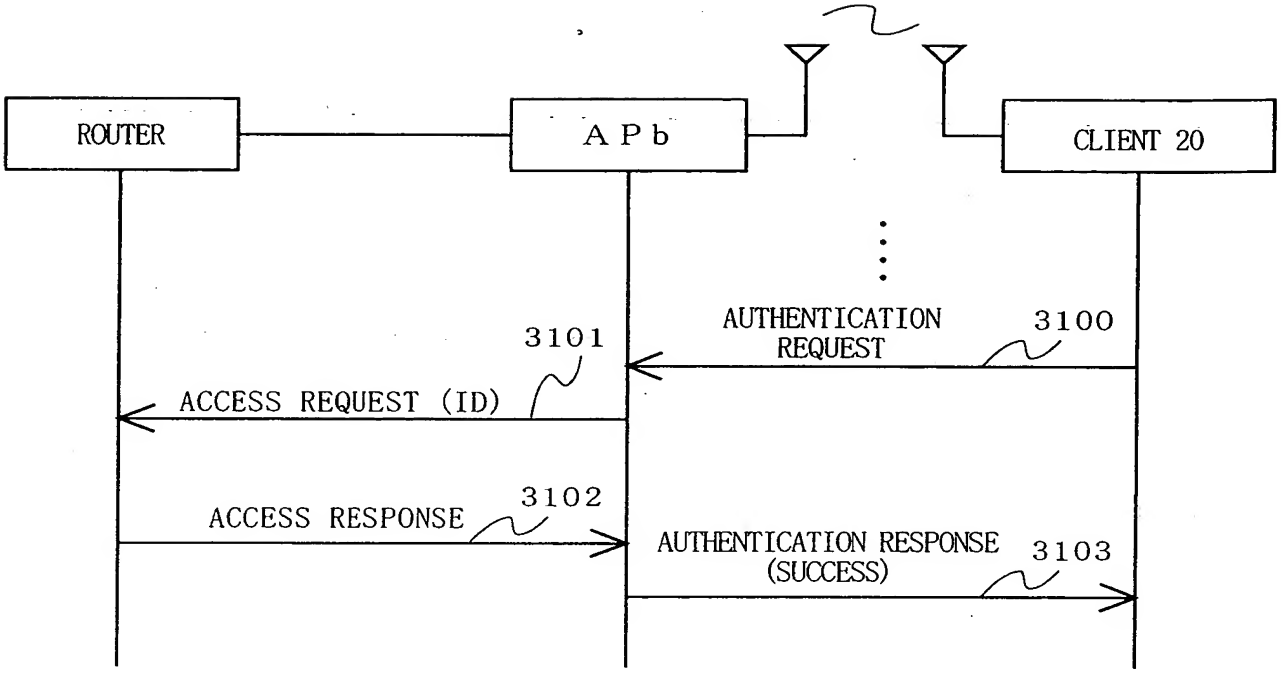

ROUTER
APb
CLIENT 20
AUTHENTICATION REQUEST
3100
3101
ACCESS REQUEST (ID)
ACCESS RESPONSE
3102
AUTHENTICATION RESPONSE (SUCCESS)
3103

FIG. 32

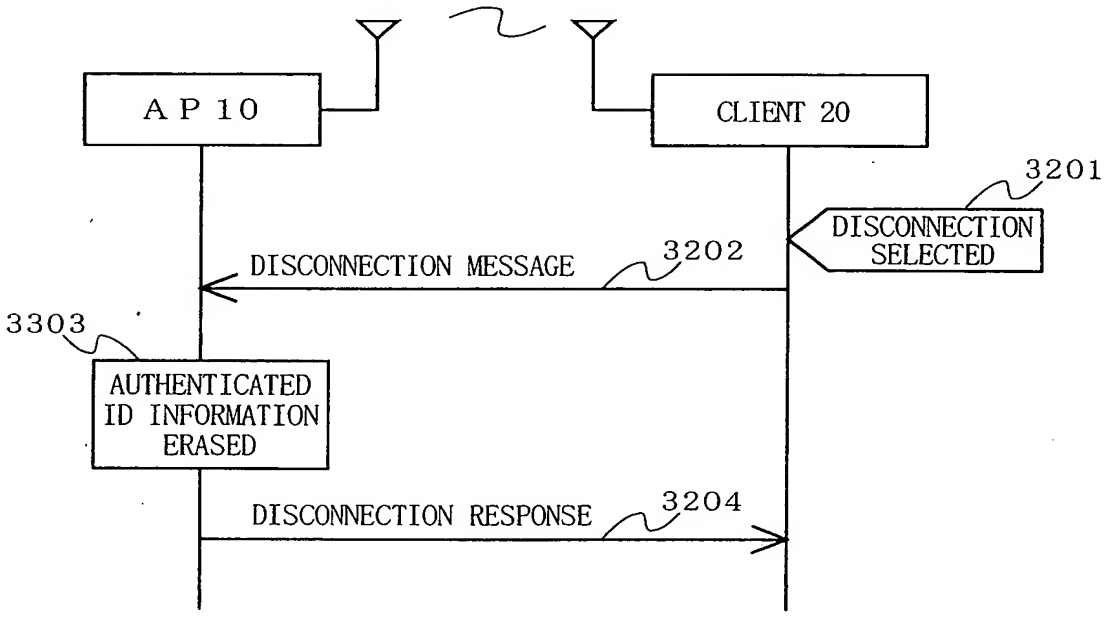

AP 10
CLIENT 20
3201
DISCONNECTION SELECTED
DISCONNECTION MESSAGE
3202
3303
AUTHENTICATED ID INFORMATION ERASED
DISCONNECTION RESPONSE
3204

FIG. 33

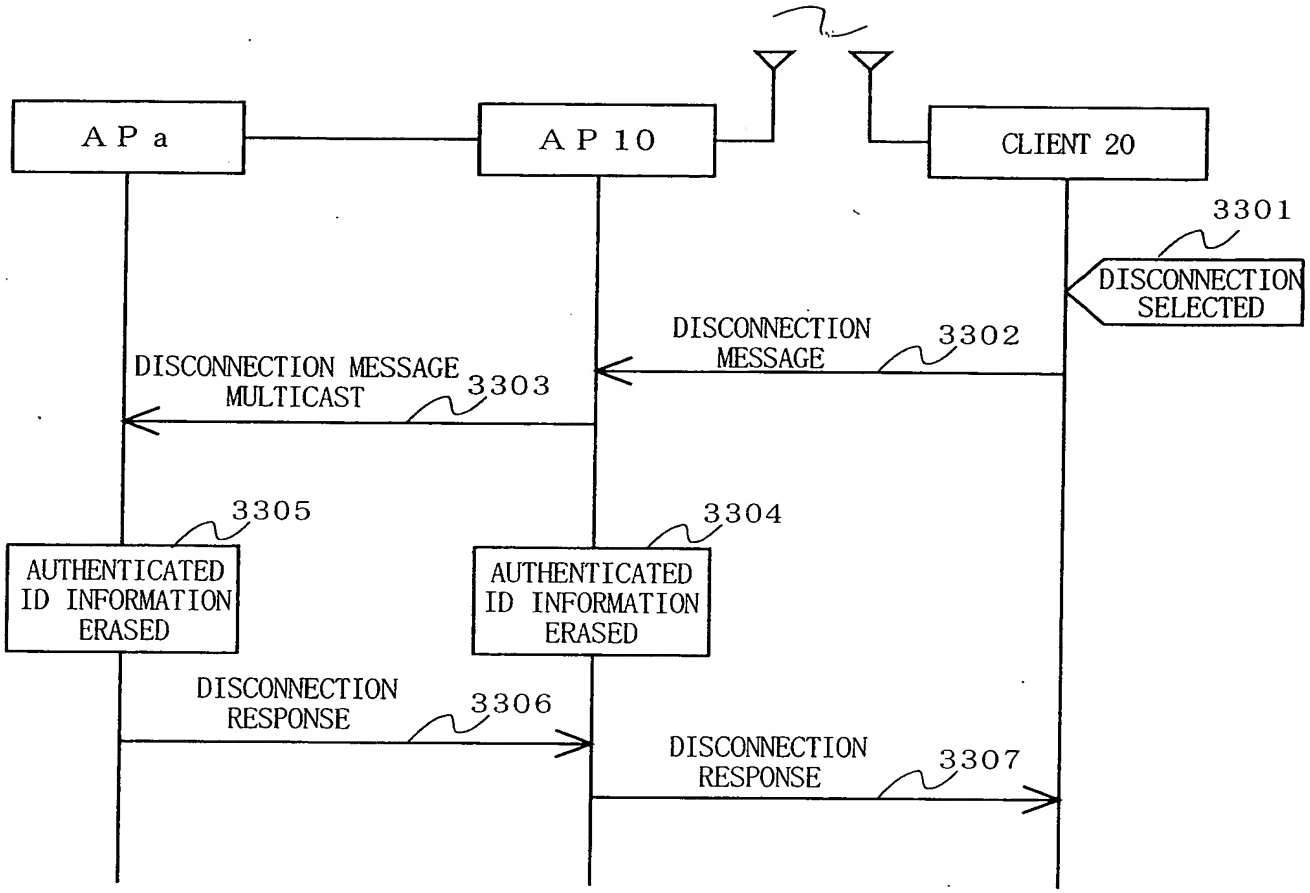

AP a
AP 10
CLIENT 20
3301
DISCONNECTION SELECTED
DISCONNECTION MESSAGE
3302
DISCONNECTION MESSAGE MULTICAST
3303
3305
3304
AUTHENTICATED ID INFORMATION ERASED
AUTHENTICATED ID INFORMATION ERASED
DISCONNECTION RESPONSE
3306
DISCONNECTION RESPONSE
3307

FIG. 34

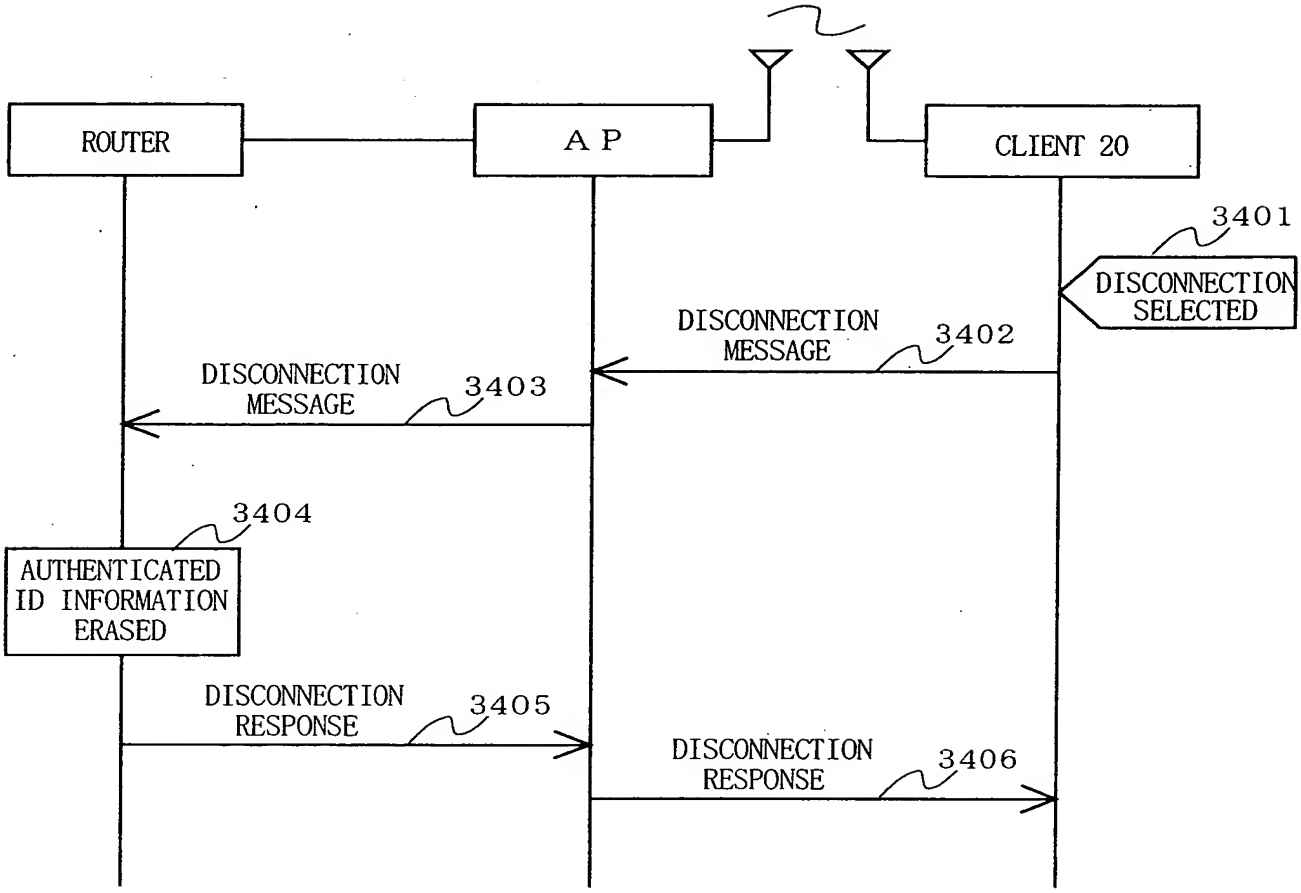

ROUTER
AP
CLIENT 20
3401
DISCONNECTION SELECTED
DISCONNECTION MESSAGE
3402
DISCONNECTION MESSAGE
3403
3404
AUTHENTICATED ID INFORMATION ERASED
DISCONNECTION RESPONSE
3405
DISCONNECTION RESPONSE
3406

FIG. 35

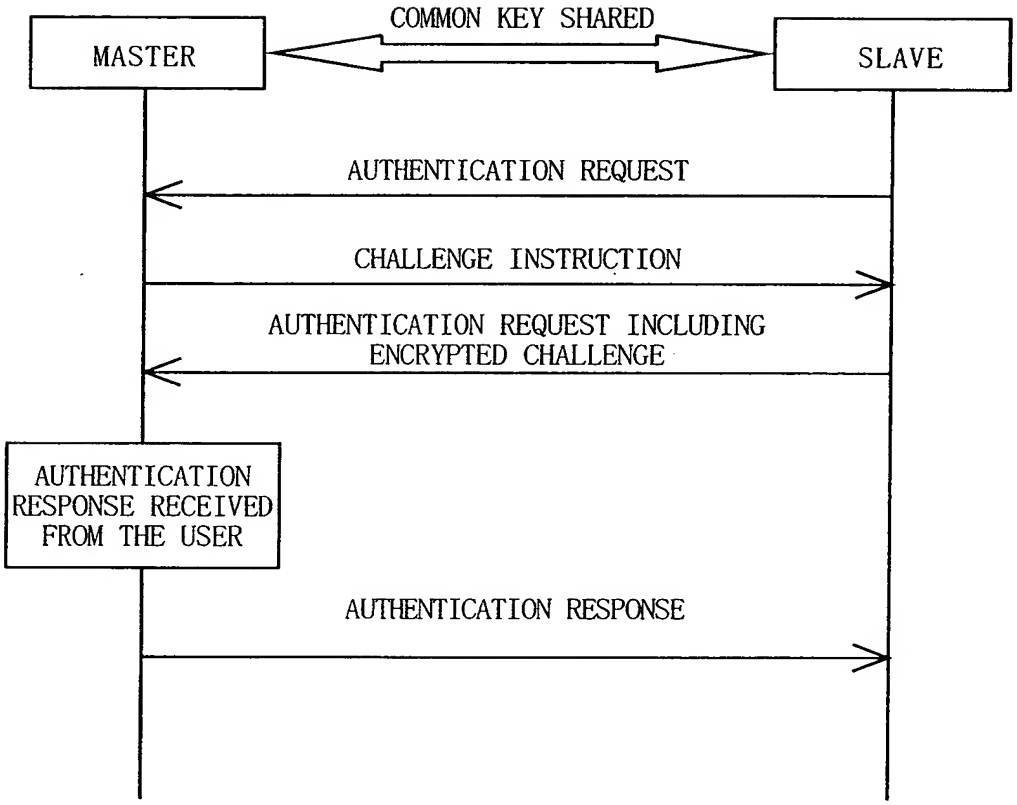

COMMON KEY SHARED
MASTER
SLAVE
AUTHENTICATION REQUEST
CHALLENGE INSTRUCTION
AUTHENTICATION REQUEST INCLUDING ENCRYPTED CHALLENGE
AUTHENTICATION RESPONSE RECEIVED FROM THE USER
AUTHENTICATION RESPONSE

FIG. 36

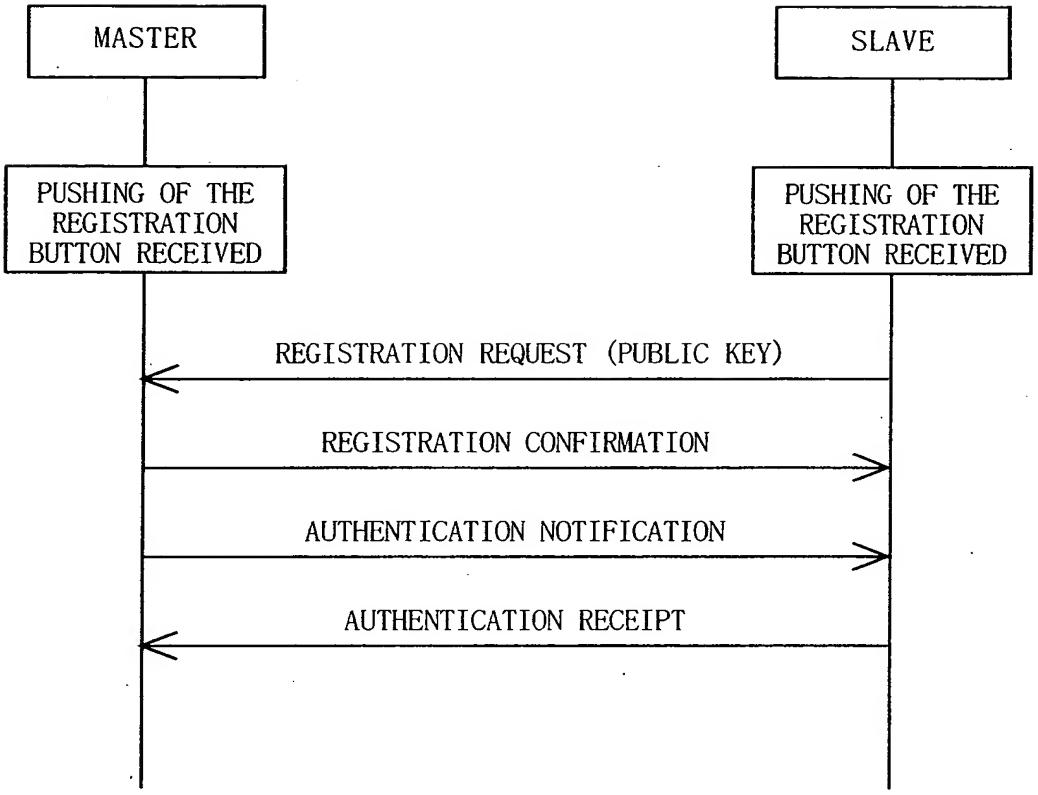
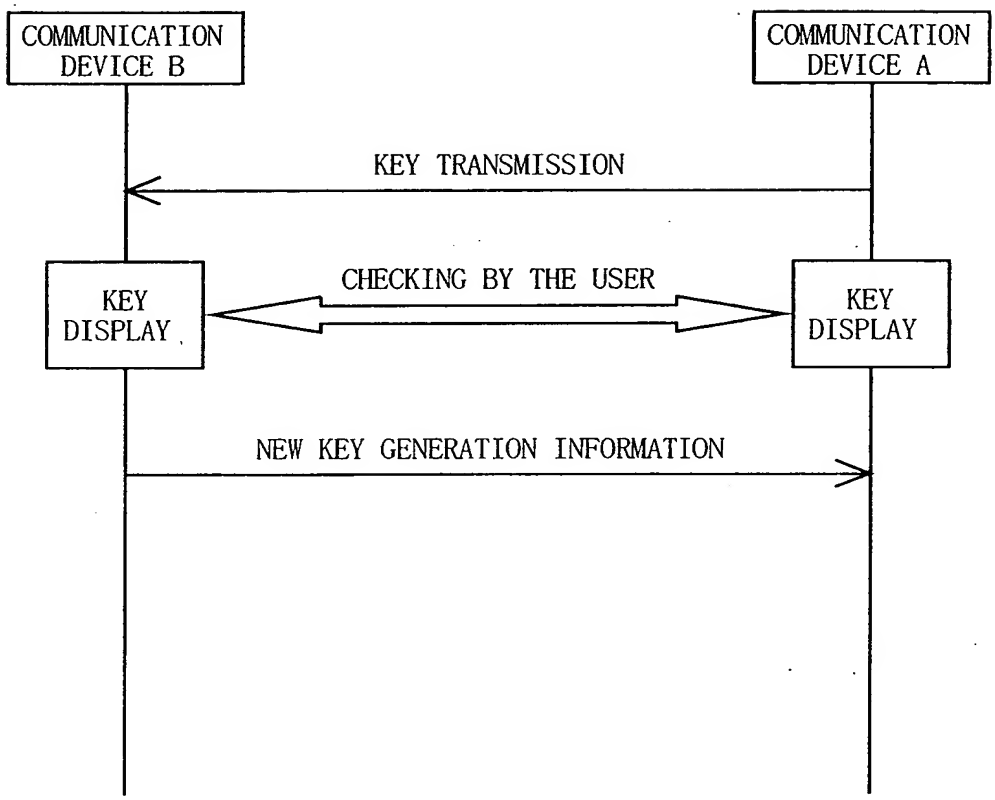

MASTER
SLAVE
PUSHING OF THE REGISTRATION BUTTON RECEIVED
PUSHING OF THE REGISTRATION BUTTON RECEIVED
REGISTRATION REQUEST (PUBLIC KEY)
REGISTRATION CONFIRMATION
AUTHENTICATION NOTIFICATION
AUTHENTICATION RECEIPT

FIG. 37


COMMUNICATION DEVICE B
COMMUNICATION DEVICE A
KEY TRANSMISSION
KEY DISPLAY
CHECKING BY THE USER
KEY DISPLAY
NEW KEY GENERATION INFORMATION